UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/987,912	11/16/2001	Mark Crosbie	10012172	7899

7590 03/18/2005

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
DODDS, HAROLD E	

ART UNIT	PAPER NUMBER
2167	

DATE MAILED: 03/18/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/987,912	CROSBIE ET AL.	
	Examiner	Art Unit	
	Harold E. Dodds, Jr.	2167	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 November 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 November 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

2. Claims 1-16 and 19-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Duval et al. (U.S. Patent No. 4,742,447), Cornelius et al. (U.S. Patent No. 6,629,081), and Curry et al. (U.S. Patent No. 6,105,013).

3. Duval renders obvious independent claim 1 by the following:

"...storing system call parameters or data the parameters point to..." at col. 18, lines 1-3, col. 18, lines 66-68, col. 19, line 1, and col. 16, line 10-11.

"...at the beginning of a system call..." at col. 7, lines 53-58, col. 18, lines 66-68, and col. 19, line 1.

"...at the end of the system call path..." at col. 16, lines 36-39, col. 18, lines 66-68, col. 19, line 1, and col. 2, lines 59-64.

Duval does not teach triggering data delivery, generating and depositing audit records, and using circular buffers.

4. However, Cornelius teaches triggering data delivery, and generating and depositing audit records as follows:

"...and triggering data delivery..." at col. 179, lines 57-59.

"...and generating an audit record and depositing the audit record..." at col. 116, lines 37-40, col. 82, lines 39-41, and col. 97, lines 3-6.

It would have been obvious to one of ordinary skill at the time of the invention to combine Cornelius with Duval to initiate data delivery at the start of a system call and maintain audit information at the end of the system call in order to have a structured procedure for processing system calls and gain wider acceptance of the system. Duval and Cornelius teach related applications. They teach the use of computers, the use of data structures, the use of parameters, the use of system calls, the use of directories, the storing of data, the accessing of data, and the use of pointers. Duval provides system calls and Cornelius provides triggering of data delivery and audit records.

Cornelius does not teach the use of circular buffers.

5. However, Curry teaches the use of circular buffers as follows:

"...in a circular buffer..." at col. 4, lines 39-41.

It would have been obvious to one of ordinary skill at the time of the invention to combine Curry with Duval and Cornelius to use circular buffers in order to provide a

means of storing information as a first-in first-out queue, which is of constant size and does not grow larger. Duval, Cornelius, and Curry teach related applications. They teach the use of computers, the use of data structures, the use of parameters, the use of directories, the storing of data, and the accessing of data and Cornelius and Curry teach the use of databases, the use of networks, and the use of audits. Duval provides system calls, Cornelius provides triggering of data delivery and audit records, and Curry provides circular buffers.

6. As per claim 2, the "...each system call...," is taught by Duval at col. 18, lines 66-68 and col. 19, line 1,

the "...that accesses files...," is taught by Cornelius at col. 151, lines 35-38,

and the "...storing related file information...," is taught by Cornelius at col. 149, lines 32-36 and col. 155, lines 35-38.

7. As per claim 3, the "...related file information...," is taught by Cornelius at col. 149, lines 32-36 and col. 155, lines 35-38,

the "...includes file owner or group...," is taught by Cornelius at col. 209, lines 25-28 and col. 57, lines 20-23,

the "...and the file information is stored...," is taught by Cornelius at col. 155, lines 35-38 and col. 149, lines 32-36,

and the "...before any modifications occur that might affect the file information...," is taught by Cornelius at col. 152, lines 48-50, col. 46, lines 48-51, and col. 155, lines 35-38.

8. As per claim 4, the "...system call parameters...," is taught by Duvall at col. 18, lines 66-68 and col. 19, line 1

and the "...that include path name parameters are stored with full path name information...," is taught by Duval at col. 2, lines 50-54, col. 3, lines 66-68, col. 4, lines 1-3, and col. 19, lines 36-40.

For claim 4, the term "entire" is used to suggest the term "full".

9. As per claim 5, the "...the audit record is a tokenized audit record...," is taught by Cornelius at col. 167, lines 56-59 and col. 97, lines 3-6.

10. As per claim 6, the "...reading audit records...," is taught by Cornelius at col. 82, lines 55-56 and col. 97, lines 3-6

and the "...from the circular buffer...," is taught by Curry at col. 4, lines 39-43.

11. As per claim 7, the "...reading is triggered...," is taught by Cornelius at col. 82, lines 55-56 and col. 179, lines 57-59

and the "...using a device read call...," is taught by Duvall at col. 5, lines 14-17 and col. 3, lines 66-68.

12. As per claim 8, the "...maintaining system wide configuration related data structures...," is taught by Cornelius at col. 89, lines 14-18 and col. 102, lines 51-52

and the "...and setting selection masks based on such structures..." is taught by Cornelius at col. 153, lines 21-25, col. 137, lines 13-15, and col. 102, lines 51-52.

13. As per claim 9, the "...collecting data...," is taught by Cornelius at col. 70, lines 18-19,

the "...in the system call path...," is taught by Duvall at col. 18, lines 66-68, col. 19, line 1, and col. 2, lines 59-64,

and the "...and formatting the collected data into an audit record...," is taught by Cornelius at col. 120, lines 14-16, col. 70, lines 18-19, and col. 97, lines 3-6.

14. As per claim 10, the "...collected data is a token stream...," is taught by Cornelius at col. 70, lines 18-19, col. 167, lines 56-59, and col. 217, lines 42-44.

15. As per claim 11, the "...if the circular buffer is full...," is taught by Curry at col. 4, lines 39-41 and col. 14, lines 48-50,

the "...then either reading some of the audit records...," is taught by Cornelius at col. 82, lines 55-56 and col. 97, lines 3-6,

the "...from the circular buffer...," is taught by Curry at col. 4, lines 39-41,

the "...or dropping new records until space becomes available...," is taught by Cornelius at col. 163, lines 1-2, col. 163, lines 29-32, and col. 150, lines 4-6,

and the "...in the circular buffer...," is taught by Curry at col. 4, lines 39-41.

16. As per claim 12, the "...maintaining root and current directions...," is taught by Cornelius at col. 156, lines 31-33, col. 157, lines 57-58, and col. 72, lines 55-61,

the "...while threads are in the middle...," is taught by Cornelius at col. 17, lines 6-11 and col. 173, lines 13-18,

and the "...of system call processing...," is taught by Cornelius at col. 216, line 16 and col. 115, lines 34-36.

17. As per claim 13, the "...selecting which data to collect before said collecting step...," is taught by Cornelius at col. 180, lines 11-22, col. 70, lines 18-19, and col. 43, lines 31-34.

18. As per claim 14, the "...said selecting step can be based on process, user, group...," is taught by Cornelius at col. 180, lines 11-22, col. 115, lines 34-36, col. 40, lines 25-30, and col. 51, lines 20-33,
the "...filename information...," is taught by Duvall at col. 2, lines 25-26,
and the "...and/or time intervals...," is taught by Cornelius at col. 160, lines 26-27.

19. As per claim 15, the "...detecting hard link accesses to a critical file...," is taught by Cornelius at col. 40, lines 46-49, col. 23, lines 7-12, col. 151, lines 35-38, and col. 150, lines 45-48.

20. As per claim 16, the "...maintaining a critical file list for monitoring hard links...," is taught by Cornelius at col. 15 , lines 45-48, col. 46, lines 45-48, col. 45, lines 12-13, and col. 23, lines 7-12.

21. As per claim 19, the "...presenting deposited data to a user space via a device driver in the kernel...," is taught by Duvall at col. 17, lines 56-58, col. 3, lines 40-42, col. 5, lines 14-17, and col. 2, lines 21-23.

22. As per claim 20, the "...configuring which system calls are audited...," is taught by Cornelius at col. 55, lines 19-21, col. 216, line 16, and col. 97, lines 3-6
and the "...by making ioctl() (control) calls on a device driver...," is taught by Duvall at col. 10, lines 38-41, col. 18, lines 66-68, col. 19, line 1, and col. 5, lines 14-17.

23. As per claim 21, the "...enabling the generation of audit data...," is taught by Cornelius at col. 61, lines 53-56, col. 116, lines 37-40, and col. 97, lines 3-6,

the "...when a device driver is opened for read...," is taught by Duvall at col. 5, lines 14-17 and col. 3, lines 31-34,

the "...and halting data generation...," is taught by Cornelius at col. 146, lines 51-53 and col. 116, lines 37-40,

and the "...when the device driver is closed...," is taught by Duvall at col. 5, lines 14-17 and col. 7, lines 17-18.

24. Claims 17 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Duval, Cornelius, and Curry as applied to claims 5 and 13 above respectively, and further in view of Cahill (U.S. Patent No. 6,535,855).

As per claim 17, the "...the tokens are either primitive or composed...," is not taught by either Duval, Cornelius, or Curry.

However, Cahill teaches the use of primitive and composed tokens as follows:

"...(Security in this situation can be established by the use of a onetime password or challenge response password device token in the possession of the customer)..." at col. 27, lines 10-13.

"...The primitive subjects of a metanetwork are 1) the Sender and Receiver/Responder as communicating persons and or entities and 2) the Message (i.e. the "application layer" content of a message or its meaning)..." at col. 58, lines 11-14.

"...The Push Packager 70 takes the text message components, the customer identification information, and the scanned data and composes a full Push message, which is then passed to the PAF Communications Component 64 for further formatting and transmission in priority order..." at col. 18, lines 7-11.

It would have been obvious to one of ordinary skill at the time of the invention to combine Cahill with Duval, Cornelius, and Curry to use either primitive or composed tokens in order to provide flexibility in defining the tokens used for communication and gain greater acceptance of the system. Duval, Cornelius, Curry, and Cahill teach related applications. They teach the use of computers, the use of data structures, the use of directories, the storing of data, and the accessing of data, Cornelius, Curry, and Cahill teach the use of databases, the use of networks, and the use of audits, and Duval, Cornelius, and Cahill teach the use of system calls and the use of pointers. Duval provides system calls, Cornelius provides triggering of data delivery and audit records, Curry provides circular buffers, and Cahill provides primitive and composed tokens.

25. As per claim 18, the "...said selecting step...," is taught by Cornelius at col. 180, lines 11-22,

the "...can be based on the outcome of system calls...," is taught by Cahill at col. 6, lines 62-65, col. 18, lines 66-68, and col. 19, line 1,

and the "...including pass, failure or both...;" is taught by Cahill at col. 19, lines 21-26 and col. 24, lines 58-61.

Conclusion

26. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Harold E. Dodds, Jr. whose telephone number is (571)-272-4110. The examiner can normally be reached on Monday - Friday 8:00 - 4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John E. Breene can be reached on (571)-272-4107. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Harold E. Dodds, Jr.
Patent Examiner
March 11, 2005